Sent by email to datasharingcode@ico.org.uk

Data sharing code consultation
Parliament & Government Affairs
Information Commissioner's Office
Wycliffe House
Water Lane
Cheshire
SK9 5AF

9th September 2019

Dear Sir/Madam,

ICO consultation on the draft data sharing code of practice

Gemserv welcomes the opportunity to respond to this consultation and thanks the Information Commissioner's Office for consulting on the updated draft data sharing code of practice.

We are an expert provider of professional services in a world driven by data and technology. Our response draws heavily from our unique insights and experience gained from delivering data governance services (including data protection, GDPR, assurance, ethics, IoT, cyber security and the Network and Information Security Directive) across the healthcare, utilities, construction and other sectors.

Please see our full response in the appendix. In summary:

- We have suggested a number of improvements to the draft Code of Practice. These include: addressing requirements around data breach notification; introducing ethical considerations in the context of data sharing; extending the scope of data sharing agreements; specific considerations regarding the sharing of children's data; international data transfers; risk assessments; due diligence considerations; and further information related to data brokers and guidance on notification to data subjects. We would encourage the ICO to include these points in the final version.

- We also believe it would be beneficial to include more information on the assignment of liability and duties between parties, depending on the joint or separate controller relationship.

- While the draft Code covers risks and issues around data sharing in detail, it could be improved by more specifically highlighting the benefits of data sharing and how this can create value for organisations.

Please do contact us if we can support you in your work, share our thoughts and ideas and answer any questions you may have with regards to our response.

Yours faithfully,

[redacted]

Gemserv Limited, Registered in England and Wales. No. 4419878
8 Fenchurch Place, London, EC3M 4AJ
T: +44 (0) 207 090 1000
F: +44 (0) 207 090 1001
W: www.gemserv.com

Appendix: Gemserv response to ICO consultation on the draft data sharing code of practice

Q1 ***Does the updated code adequately explain and advise on the new aspects of data protection legislation which are relevant to data sharing?***

☐ ***Yes***

☒ ***No***

Q2 ***If not, please specify where improvements could be made.***

The updated draft Code addresses and provides guidance on the responsibilities of the parties engaged in data sharing. In addition, it covers many of the new and updated challenges raised by the GDPR, such as the need to conduct Data Protection Impact Assessments on data sharing between sharing parties and enhanced individual rights.

The updated draft Code could more specifically address requirements around data breach notification, including the responsibilities between the parties. Although this is not an explicit requirement in relation to joint controllership, it is increasingly becoming best practice to include clauses specifying responsibility for notifying the other party, in addition to specifying the circumstances when each party will be responsible for notifying other supervisory authorities, etc. In the case of data sharing between separate data controllers, the lack of such requirements may also cause issues.

We also discuss several other improvements below, including to specifically include references to ethical considerations in the context of data sharing, data sharing agreements, sharing of children data, international data transfers, risk assessments, due diligence considerations and further information on data brokers and guidance on notification to data subjects.

Q3 ***Does the draft code cover the right issues about data sharing?***

☐ ***Yes***

☒ ***No***

Q4 ***If not, what other issues would you like to be covered in it?***

In our opinion, the Data Sharing Code should be revised to include specific requirements to examine wider ethical and reputational risks around data sharing. For example, as we have recently seen with the Cambridge Analytic scandal, organisations should be made aware that engaging with data sharing partners who are involved in disreputable practices (such as non-transparent data processing, collection or data mining without consent, sourcing data from illicit locations) can stigmatise both organisations involved. Ensuring that personal data is going to be collected or shared in a legal and ethical way (including within the reasonable expectation of data subjects) is vital as third parties may be a source of reputational risk in addition to a security or compliance risk. This should be included in the requirements to conduct Data Protection Impact Assessments (DPIA) into data sharing that the ICO is outlining organisations should take.

As part of the Code, organisations involved in joint campaigns should examine the ethics and values of the recipient organisation, in the course of any risk assessment. On top of the usual data security and limitations on processing, and data processing assurances, that should be ascertained between organisations prior to engaging in data sharing, the initial assessment should extend to investigating whether any complaints have been lodged or negative media coverage of such potential partners. Additionally, organisations should also seek to see proof of transparency notices or codes of conduct that partnering organisations have committed to, particularly those engaging in data analytics or profiling.

In addition, we would consider it particularly valuable if the ICO could produce guidance applicable to political parties, including around data sharing for campaigning of political advertising purposes. Lastly, in 2018, the ICO conducted a review of data sharing between political parties, including data used for microtargeting, which raised a lot of concerns. In particular, further guidance in the draft Code should focus on sorts of profiling (including automated decision-making) that should be prohibited and limitations of the ability to combine data sets (including public sources) to target individuals.

Moreover, we would consider it to be particularly helpful if the ICO could produce more specific guidance on requirements for data sharing agreements by differentiating those in agreements between joint data controllers and separate data controllers. More specifically, by highlighting how contractual arrangements and obligations would differ in both instances, for example, in relation to carrying out of DPIAs, notification of data breaches, response to data subjects' requests, this would aid parties in taking adequate measures needed to address the relevant liabilities and remain compliant.

Q5 Does the draft code contain the right level of detail?

☐ ***Yes***

☒ ***No***

Q6 If no, in what areas should there be more detail within the draft code?

The Code provides a suitable skeleton framework with regards to data security, and notices to data subjects, enabling organisations to easily follow and abide by it. It also covers all of the key areas to some degree – including data sharing agreements, data security, transparency and staff training, among others.

However, we are of the opinion that it would be beneficial to have more information on the assignment of liability and duties between the parties, depending on the joint or separate controller relationship. This could be supplemented with case studies, – for example, describing the data sharing situations in which each of these relationships would arise. Additionally, we would like the code to cover more specific questions, such as the requirements for determining the lawful basis in case of data sharing between separate data controllers (i.e. it might be the case that lawful basis may not be commonly used and may require further consideration). Moreover, particularly where joint controllers are using the same database, data security requirements or arrangements, and requirements with respect to ensuring the accuracy of data should also be further substantiated.

On top of this, guidance around the use of data broker in data sharing is to some degree included in the Code – particularly around controls on the use of publicly available data or data from public sources and ensuring the transparency and reasonable expectations of data subjects around this, such as checking how it was initially collected. Again however, further detail could be helpfully included such as on obligations to assess - for example through a DPIA - whether information has been repurposed during data sharing.

Separately, the Code would also add value by outlining where and when (for example, in Privacy Notices), data subjects should be informed of which parties and which data will be subject to data sharing. Although this is mentioned briefly in the section on transparency requirements, the fact that a list of parties with whom data will be shared and a link to their Privacy Notices/Policies, for example, is now best practice but is not recommended in the Code,. Moreover, guidance on data sharing in other jurisdictions, such as in relation to the French Data Protection Authority (CNIL) has specified that organisations update data subjects when parties to the data sharing changes.

Additionally, we would like to see more guidance in relation to data sharing for data modelling; how data shared for data pooling should be treated when the data-sharing agreement ceases; and how any legacy or unnecessary data should be treated in case of data sharing for mergers and acquisitions.

Finally, we believe that more specific guidance in relation to the responsibility to obtain consent for sharing of children's personal data would add value, in particular, because this is a frequent issue at schools and is difficult to implement due to the legal guardians involved, who will need to be informed of the data sharing and may even be required to provide consent.

Q7 Has the draft code sufficiently addressed new areas or developments in data protection that are having an impact on your organisation's data-sharing practices?

☐ ***Yes***

☒ ***No***

Q8 If no, please specify what areas are not being addressed, or not being addressed in enough detail.

The code has not sufficiently addressed technological developments with regards to online advertising. In particular, it would help to elaborate on issues related to data collected by certain platforms or on certain websites or providers (such as, for example, using cookies) being shared with further parties without sufficient notice and consent. When combined with difficulties the ICO (and other European supervisory authorities such as the CNIL in France) are attempting to overcome with regard to adequate consent frameworks for data collected through cookies, further data sharing requirements with respect to the exchange of information between parties in an online advertising chain becomes necessary.

Moreover, detail on data transfers outside of the EU/EEA, and onward transfers to other companies could be provided – and what the sharing organisation should demand from them (with regard to assurances around data protection and data security) depending on where the data is being transferred to. For example, transfers from a UK entity to the USA and then beyond under the Privacy Shield should involve organisations being obliged to allow individuals to opt-out from the onward transfer, unless needed for a core service provider (which is likely to exclude most instances of data sharing). These circumstances and the limitations on data sharing they provide should be further substantiated.

Also, although the draft Code does go into detail on the requisite elements to include in carrying out Data Protection Impact Assessments (DPIAs), this could be further developed with the inclusion of elements such as the need to more broadly consider factors relevant to impact assessments of data sharing. For example, organisations could look at whether the sharing with an additional third party is necessary – what value will they add, and can existing expertise in-house be used? Furthermore, a full plan for the data sharing lifecycle should be put into place, including considerations with regards to which party will have ownership of relevant assets and resourced, and where data will be moved to or processed if or when the data sharing ends.

Additionally, due diligence in the context of mergers and acquisitions is not appropriately addressed. For example, the Data Sharing Code lacks specific provisions for organisations to risk assess organisations

assimilated in the course of mergers and acquisitions. In our opinion, the Data Sharing Code should include further guidance on conducting due diligence on such organisations during the M & A procedure. As such, before data sharing, an organisation should risk-assess any third parties from which it collects or shares data, including those acquired through mergers and acquisitions.

There is existing content in the Data Sharing Code addressing these issues, including the need to ensure that the recipient (e.g. third party) is aware of the sensitivity of the data being acquired, that security risks that could result in a loss of degradation or personal data during sharing are identified, that records of data are accurate and a retention policy is in place. However, this advice is largely directed to an organisation being acquired – rather than an acquiring company risk-assessing a supplier or a target company due to be acquired.

As such, more detail should be developed around data security measures in place, data collection methods and any other high-risk third-party contractors, which should be included in the Data Sharing Code. This would allow it to better address the wider reputational and operational risk involved in acquiring parties in the course of mergers and acquisitions. Such risks can manifest themselves in the form of data breaches that remain uncovered – as Marriott encountered when acquiring Starwood Group in 2016, and subsequently discovering a data breach extending to 339 million records, on Starwood's systems, which had occurred since 2014. In such a situation, due diligence should include to risk assess such organisations. This is particularly the case with respect to data that is received or otherwise acquired from companies during a merger or acquisition, particular where the companies' systems will be integrated and where data will be transferred between the parties.

For example, when conducting a due diligence assessment, the following requirements or guidance could also be relevant to organisations:

- Conducting in-depth data mapping activities of an acquired entities information flows, including assessing insecure locations where personal data could be stored or collected from, and identifying data flows and transfers where information may be at risk;
- Identifying any assessments of information and network security and vulnerabilities, and any system records of previous security incidents or breaches and the relevant action taken;
- Examining the existence of governance and procedures for incident management and data breach notification – including whether staff and relevant audits or checks are in place;
- Identifying any sub-contractors supporting the acquired entity (either in providing support or from whom data is sourced) have been assessed from a risk perspective, including whether they underwent a due diligence process in terms of their security risks, whether their staff are committed to confidentiality, and which limits are placed on which data they have access to and limitations on how it is used. Additionally, ethical and reputational risks should also be identified – including whether any sub-contractors that have been on-boarded have attracted any negative media coverage or whether they do not meet the requisite ethical and transparent standards for collecting and using data.

In particular, the absence of any governance or self-assessment conducted by the organisation should raise an immediate red flag.

Q9 ***Does the draft code provide enough clarity on good practice in data sharing?***

☐ ***Yes***

☒ ***No***

Q10 ***If no, please indicate the section(s) of the draft code which could be improved and what can be done to make the section (s) clearer.***

The draft code is easy to follow without expert knowledge of data protection and there are plans to incorporate checklists which should facilitate comprehension. Moreover, the use of specific 'FAQ' examples, such as resolving misconceptions that consent is always needed in relation to data sharing, is very helpful to help solve organisations' immediate concerns.

The examples in Annex D, which include sector-specific guidance, are very useful for organisations to practically implement. However, these could be expanded, and some improvements could include those specific to the online advertising industry, where issues around using data brokers, using platforms and services such as Facebook's Custom Audiences could be discussed further.

Additionally, the code could provide more fit for purpose requirements for data sharing agreements. For example, "the benefits you hope to bring to individuals or to society more widely" seem to sit better in a DPIA or LIA rather than in a contract. A data protection policy could be suggested to be appended to the agreement and serve as a measure to ensure the same level of compliance by data controllers.

Q11 Does the draft code strike the right balance between recognising the benefits of sharing data and the need to protect it?

☐ ***Yes***

☒ ***No***

Q12 If no, in what way does the draft code fail to strike this balance?

Although the draft Code covers the risks and issues around data sharing in detail, it could do better by more specifically covering the benefits of data sharing and how it could bring more value to organisations

In order to better describe the benefits, specific use cases in industries need to be described in more detail. In particular, data sharing can form part of a useful project for organisations, particularly around allowing better use to be made of that data with analytics capabilities in other organisations. New examples could be provided that highlight the benefit in specific sectors, such as that, in the health care sector, for example, data sharing with researchers and even technology organisations involved in training AI healthcare solutions allows investigations into better treatment and diagnosis of conditions. The key issues that the code should focus on are i) whether the data needs to be personally identifiable for the purpose of the sharing, and; ii) what data minimisation measures can be put into place to maintain the benefits of the sharing while reducing the risks for individuals.

For example, this could involve two NGOs engaged in a campaign sharing lists of activists, or two retailers offering combined products on a promoted offer that are sharing customers' contact details from those who have consented to data sharing. Describing the benefits to the sharing parties and also to data subjects (for example, in receiving product offers relevant to them), would also help an organisation in terms of identifying, as part of a legitimate interest test, the legitimate business interests of the sharing parties and individuals.

Q13 Does the draft code cover case studies or data sharing scenarios relevant to your organisation?

☒ ***Yes***

☐ ***No***

Q14 Please provide any further comments or suggestions you may have about the draft code.

We have no further comments.

Q15 ***To what extent do you agree that the draft code is clear and easy to understand?***

☐ ***Strongly Agree***

☒ ***Agree***

☐ ***Neither agree nor disagree***

☐ ***Disagree***

☐ ***Strongly Disagree***

Q16 ***Are you answering as:***

☐ ***An individual acting in a private capacity (e.g. someone providing their views as a member of the public)***

☐ ***An individual acting in a professional capacity***

☒ ***On behalf of an organisation***

☐ ***Other***

Gemserv

9th September 2019